


Security Target for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406



Issue : 1.7
Date : 22 June 2009
Status : Definitive

Distribution : Consultancy File, CLEF, Joel Crisp, Ann Craig, CESG

Prepared by :  Hugh Griffin
Rizwan Arshad

Reviewed by : Steve Hill

Authorised by : Peter Goatly

=====

Security Target for Oracle Business Intelligence Enterprise Edition 10g (10.1.3.3.2) with Quick Fix 090406

June 2009

Authors: Hugh Griffin and Rizwan Arshad.

Contributors: Ann Craig and Joel Crisp.

Copyright © 2009, Oracle Corporation. All rights reserved. This documentation contains proprietary information of Oracle Corporation; it is protected by copyright law. Reverse engineering of the software is prohibited. If this documentation is delivered to a U.S. Government Agency of the Department of Defense, then it is delivered with Restricted Rights and the following legend is applicable:

RESTRICTED RIGHTS LEGEND

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of DFARS 252.227-7013, Rights in Technical Data and Computer Software (October 1988).

Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing.

Oracle Corporation does not warrant that this document is error free.

Oracle is a registered trademark and Oracle Business Intelligence 10g are trademarks or registered trademarks of Oracle Corporation. Other names may be trademarks of their respective owners.

=====

Document History

Version	Date	Notes
0.8	6 June 2008	Draft for Technical and Certification Body review
0.9	18 June 2008	Evaluation version after review comments incorporated
1.0	23 June 2008	Evaluation version after CB review comments finalised
1.1	01 August 2008	Evaluation version after resolution of observation reports and the completion of the High Level Design.
1.2	07 October 2008	Evaluation version after confirmation of Hardware platforms
1.3	03 December 2008	Evaluation version after resolution of evaluator observations
1.4	11 May 2009	Definitive version
1.5	01 June 2009	Typo fix
1.6	02 June 2009	Typo fix
1.7	22 June 2009	Typo fix

Table Of Contents

1	Introduction	5
1.1	Purpose.....	5
1.2	TOE Overview.....	5
1.3	CC Conformance Claim.....	6
1.4	Document Structure.....	6
1.5	Terminology.....	7
2	TOE Description	11
2.1	Physical Scope of the TOE.....	11
2.2	Logical Scope of the TOE.....	13
2.3	IT Environment for the TOE.....	18
2.4	TOE Security Architecture.....	18
3	Security Problem Definition	22
3.1	Threats.....	22
3.2	Assumptions.....	25
4	Security Objectives.....	27
4.1	TOE Security Objectives.....	27
4.2	Security Objectives for the Operational Environment.....	27
5	Security Requirements	32
5.1	Security Functional Requirements.....	32
5.2	Security Assurance Requirements.....	46
6	ST Rationale	47
6.1	Security Objectives Rationale.....	47
6.2	Security Requirements Rationale.....	50
7	Extended Components Definition	55
8	Conformance Claims	56
Annex A	Rules for Group Privilege and Permissions Inheritance	57
A.1	Rules for Inheritance in Oracle BI Presentation Services.....	57
A.2	Example of Inherited Permissions and Privileges in Oracle BI Presentation Services.....	57
Annex B	Presentation Catalog Object Types List.....	60
B.1	In scope of the TOE.....	60
B.2	Out of scope of the TOE.....	60
Annex C	62	62
C.1	DELL Optiplex 745 hardware configuration.....	62

Referenced Documents

AG_BIPS	Oracle Business Intelligence Presentation Services Administration Guide (10.1.3.2), dated December 2006
BR-DBMS	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, version 1.2, 25 July 2007
C_DB	Certification Report BSI-DSZ-CC-0403-2008, Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1, version 1.0, dated 28 January 2008
C_OEL	Certification Report BSI-DSZ-CC-0468-2007, Oracle Enterprise Linux Version 4 Update 5, version 1.0, dated 19 July 2007
C_OID	Certification Report CRP244, Oracle Internet Directory 10g (10.1.0.4.1), Issue 0.B, dated May 2008
CC	Common Criteria for Information Technology Security Evaluation (Comprising Parts 1-3: [CC1], [CC2], and [CC3])
CC1	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model CCMB-2006-09-001, Version 3.1 Release 1, September 2006
CC2	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCMB-2007-09-002, Version 3.1 Release 2, September 2007
CC3	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements CCMB-2007-09-003, Version 3.1 Release 2, September 2007
CEM	Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology CCMB-2007-09-004, Version 3.1 Release 2, September 2007
ECG	Evaluated Configuration Guide for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406, version 0.8, dated May 2009
OEL_ST	Oracle Enterprise Linux Version 4 Update 5 Security Target for CAPP compliance, version 1.6, dated 12 July 2007.

1 Introduction

1.1 Purpose

This document is the Security Target (ST) for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406.

Title: Security Target for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406

Target of Evaluation (TOE): Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406.

Release: (10.1.3.3.2) with Quick Fix 090406

Operating System Platform: Oracle Enterprise Linux, Version 4 Update 5 with the capp-eal4-config-oracle package, see EAL4 certificate [C_OEL].

Database Platform: Oracle 10g Release 2 Database Server Enterprise Edition (10.2.0.3.0), see EAL4 certificate [C_DB].

LDAP Directory Platform: Oracle 10g Internet Directory (10.1.4.0.1), see EAL4 certificate [C_OID].

Keywords: Oracle Business Intelligence Enterprise Edition, EAL3.

The role of the security target within the development and evaluation process is described in the CC: the Common Criteria for Information Technology Security Evaluation [CC].

1.2 TOE Overview

Typically, organizations track and store large amounts of data about products, customers, prices, contacts, activities, assets, opportunities, employees, and other elements. This data is often spread across multiple databases in different locations with different versions of database software. Oracle Business Intelligence Enterprise Edition (Oracle BIEE) is a suite of products that allow enterprises to manage, report on and present access to their data via a single common business model. The security features of Oracle BI ensure data integrity, and confidentiality.

Oracle BIEE is used in conjunction with the following evaluated products: Oracle Database, and Oracle Enterprise Linux. Optionally, Oracle Internet Directory can be used for authentication in the evaluated configuration.

For this evaluation of Oracle BIEE, the products that are in the Target of Evaluation are:

- Oracle Web Services (10.1.3.3.2),
- Oracle BI Presentation Services (10.1.3.3.2) with Quick Fix 090406 and
- Oracle BI Server (10.1.3.3.2) with Quick Fix 090406.

[ECG] defines how the TOE products must be installed in the evaluated configuration and defines the requirements for the setting up of the TOE environment.

The security functionality in the TOE includes:

- User identification and authentication with password management for local administrators; Oracle BIEE hands off authentication to other Oracle evaluated products like Oracle Database, or Oracle Internet Directory for normal users;
- Access Control over all Presentation Services objects accessible from the web services such as requests and queries;
- Encryption of data transmitted between components within Oracle BIEE; and from external clients to BIEE;
- User accountability.

1.3 CC Conformance Claim

The TOE conforms to the CC as follows:

- CC Part 2 extended
- CC Part 3 conformant
- EAL3 conformant
- No conformance with any Protection Profile is claimed.

1.4 Document Structure

This ST is divided into 7 sections, as follows:

- Section 1 (this section) provides an introduction to the ST.

- Section 2 provides a description of the TOE.
- Section 3 provides the security problem definition for the TOE and its environment.
- Section 4 provides the statement of security objectives, defining what is expected of the TOE and its environment, in order to solve the security problem defined in Section 3.
- Section 5 provides the statement of IT security requirements, defining the functional and assurance requirements on the TOE that are needed to achieve the relevant security objectives defined in Section 4. With each SFR or SFR group a TOE summary specification is provided. This describes how the TOE meets the SFRs.
- Section 6 provides the ST Rationale, which demonstrates that:
 - the security problem defined in Section 3 will be solved if the TOE and its environment achieves the security objectives stated in Section 4;
 - the TOE security objectives will be achieved if the TOE satisfies the security requirements in Section 5.
- Section 7 provides the Extended Components Definition.
- Annex A provides an example of group privilege and permissions inheritance in the TOE
- Annex B provides a list of all the object types that can be stored in the Presentation Catalog.

1.5 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Acronyms

ACI	Access Control Item
ACL	Access Control List
API	Application Program Interface

BI	Business Intelligence
BIEE	BI Enterprise Edition
CC	Common Criteria
CEM	Common Evaluation Methodology
CI	Configuration Item
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECG	Evaluation Configuration Document
ETR	Evaluation Technical Report
HTML	Hyper-Text Markup Language
HTTPS	Hyper-Text Transfer Protocol Secure
IEEE 1394	a serial bus interface standard , for high-speed communications and isochronous real-time data transfer known as Firewire
ISO	International Standards Organisation
IT	Information Technology
J2EE	Java 2 Enterprise Edition
OAS	Oracle Application Server
OBI	Oracle Business Intelligence
OC4J	Oracle Containers for J2EE
OCI	Oracle Call Interface
ODBC	Open Database Connectivity
OEL	Oracle Enterprise Linux
OHS	Oracle HTTP Server
OID	Oracle Internet Directory
OR	Observation Report

OSP	Organisational Security Policy
PP	Protection Profile
PCL	Printer Command Language
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TDEA	Triple DES Encryption Algorithm
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
USB	Universal Serial Bus

Terms

BI Answers	An administrator interface for configuring the business model and setting up presentation objects like requests/reports. User access is provided via the web services API.
BI Interactive Dashboards	An interface for designing dashboards. This is out of the scope of the TOE.
BI Presentation Services	The part of the TOE concerned with presenting the results of queries to the user, e.g. in reports.
BI Server	The part of the TOE concerned with providing structure to the data stored in the backend database.
Business Model	TOE specific term denoting a representation of a physical table in a database in terms of a column of data.

Chart	A graphical representation of data, e.g. a pie chart, or a bar graph.
Dashboard	A Presentation Services object that displays the result of one or more requests. Dashboards exist as XML and so can refer to and call upon many other types of information. They can be manipulated by the web services.
Filter	A Presentation Services object that constrains the results returned by a request to obtain answers to a particular business question.
Folder	A storage container in the TOE Presentation Services file system that holds other data objects. These are subject to ACLs.
Gauge	A graphical representation that displays whether data is within pre-defined limits. E.g. a dial gauge shows data using a dial with one or more indicator needles. The dial will use a metric meaningful to the user such as 'thousands of products sold'.
Link	A pointer in the TOE Presentation Services file system that points to another data object or folder. These are subject to ACLs.
Presentation Catalog	The collection of all the presentation data objects (e.g. Requests and Filters) and their access control permissions.
Report	The result returned by a request.
Repository	The collection of all BI server objects (e.g. presentation columns, presentation tables, and connection pools).
Request	A user accessible reference to a query that returns data based upon the data sources accessed. The result of executing a request is called a Report.
Subject Area	A logical grouping of data based on a subset of a business model column.
Web Services	The API through which services of the TOE are offered to end user applications.

2 TOE Description

This part of the ST provides an overview of the security capabilities of Oracle Business Intelligence Enterprise Edition (Oracle BIEE).

To this end, the TOE description discusses:

- *the physical scope of the TOE*: a list of all hardware, firmware, software and guidance parts that constitute the TOE, sufficient to give the reader a general understanding of those parts.
- *the logical scope of the TOE*: describing the logical security features offered by the TOE to a level of detail that is sufficient to give the reader a general understanding of those features. This includes a brief discussion of security features not addressed by the security functional requirements in Chapter 5.

Oracle Business Intelligence Enterprise Edition (Oracle BIEE) is a suite of products that allow enterprises to securely manage, report on and present access to their resources and assets via a single common business model. It provides users with secure, fine-grained access to enterprise resources and assets.

2.1 Physical Scope of the TOE

2.1.1 Software

For this evaluation, the Oracle BIEE software products which constitute the TOE are as follows:

- Oracle Web Services (10.1.3.3.2),
- Oracle BI Java Host (10.1.3.3.2),
- Oracle BI Answers (10.1.3.3.2),
- Oracle BI Server (10.1.3.3.2) with Quick Fix 090406, and
- Oracle BI Presentation Services (10.1.3.3.2) with Quick Fix 090406.

The latter two products incorporate OpenSSL version 0.9.8j to implement secure communications channels as part of the TOE.

The following software products are out of the scope of the TOE:

- Oracle BI Interactive Dashboards,
- Oracle BI Delivers,
- Oracle BI Marketing,
- Oracle BI Scheduler and Job Manager,
- Oracle BI Publisher.

The first three products are disabled using privilege based access controls; the latter three are not installed.

2.1.2 Firmware

Oracle BIEE does not rely on any firmware.

2.1.3 Hardware

Oracle BIEE does not rely on any hardware or peripherals. The hardware on which the TOE software is executed is considered part of the TOE environment.

The TOE is running on the following hardware platforms:

- Dell OptiPlex 745 described in Annex C.1.

The following peripherals can be used with OEL preserving the security functionality:

- all terminals supported by the OEL (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces).
- printers compatible with PostScript level 1 or PCL 4 attached via parallel port, USB, or Ethernet.
- all storage devices and backup devices supported by OEL (hard disks, CDROM drives, streamer drives, floppy disk drives) (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces).
- all Ethernet and Token-Ring network adapters supported by the OEL.

Note: peripheral devices are part of the TOE environment.

Note: Excluding hot pluggable devices connected via USB does not exclude all USB devices. USB printers, keyboards and mice may be attached provided they are connected before booting the operating system.

2.2 Logical Scope of the TOE

The major products in the Oracle BIEE architecture are described below. Its security features are described in terms of this architecture. The TOE's mechanisms for identification and authentication, access control, data exchange and user accountability are then summarised. Other Oracle BIEE security features that are not within the scope of the evaluation are also briefly discussed. These features are either not installed or excluded using access controls.

2.2.1 Overview

Typically, organizations track and store large amounts of data about products, customers, prices, contacts, activities, assets, opportunities, employees, and other elements. This data is often spread across multiple databases in different locations with different versions of database software.

After the data has been organized and analyzed, it can provide an organization with the metrics to measure the state of its business. This data can also present key indicators of changes in market trends and in employee, customer, and partner behaviour. Oracle BI helps end users obtain, view, and analyze the data. The security features of Oracle BI ensure data integrity, and confidentiality.

Figure 2.1, on the following page, shows the Oracle BIEE security architecture:

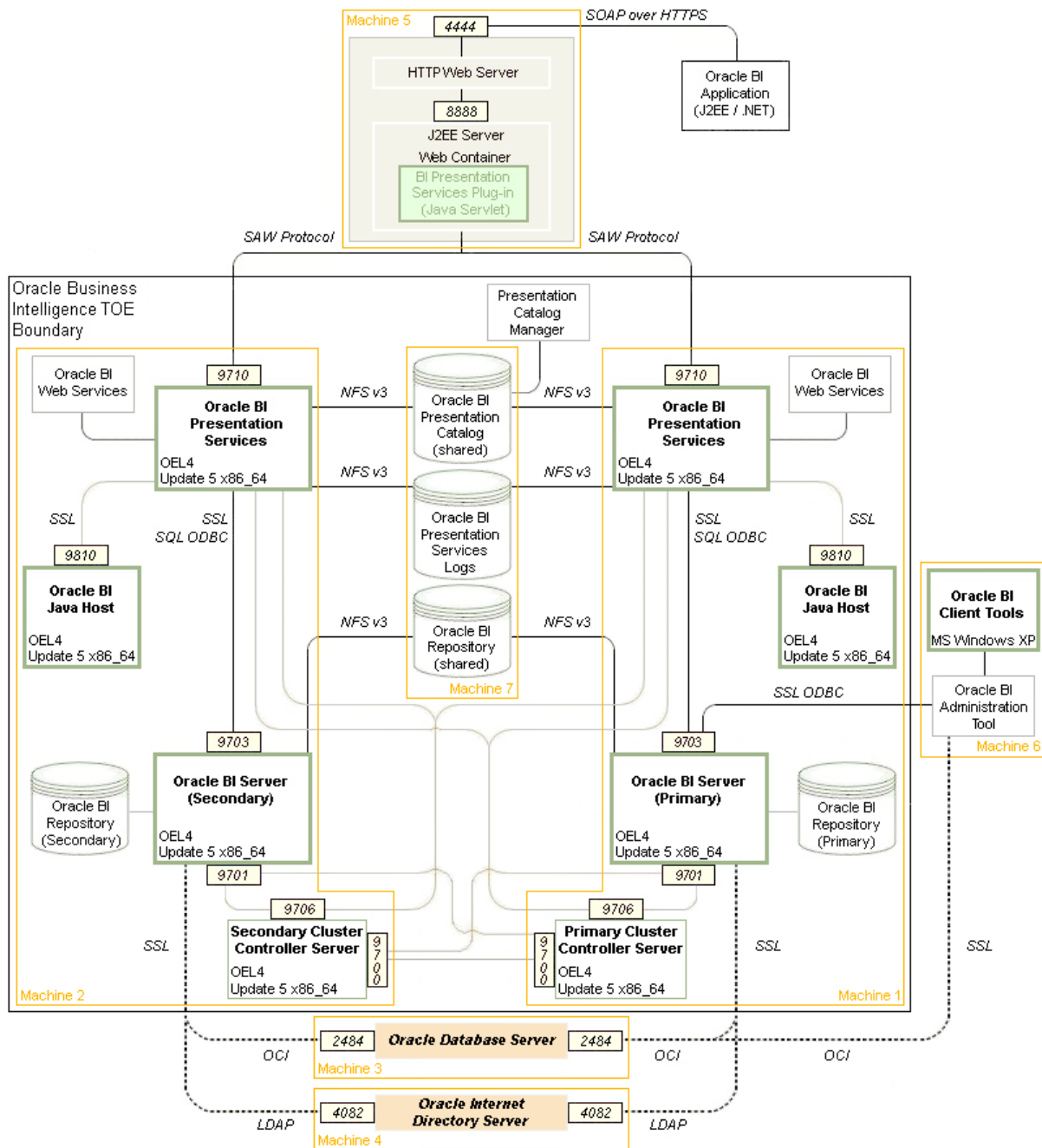


Figure 2.1: The Oracle BIEE security architecture

The numbers in boxes (e.g. 9700) in Figure 2.1 are port numbers.

The Oracle BI Administration tool and Presentation catalog manager are hosted on a Windows XP machine situated in the same physically secure location as the OEL servers.

The excluded products listed in section 2.1.1 above are either not installed or excluded using the privilege regime within the TOE, and therefore, are not shown on the diagram. The products installed are those needed to fulfil the central functionality provided by the TOE as described in section 1.2 above. A clustered configuration has been chosen as typically the size and variety of back end data sources require clustering to provide failover. It is recommended that the Network File system (NFS) is hosted on a Storage Area Network (SAN) to allow audit trail integrity in the event of failover.

There is only one mode of operation of the TOE.

2.2.2 Oracle BI Web Services

The user interface to the TOE is Oracle BI Web Services via SOAP and HTTPS. Oracle BI Web Services is an Application Programming Interface (API) that implements SOAP. It allows a user to perform the following functions:

- Authenticate to the TOE.
- Extract results from data sources using requests and queries from Oracle BI Presentation Services for that user and deliver them as reports to external applications.
- Perform Oracle BI Presentation Catalog management functions for suitably permitted and privileged users.

A capability to execute Oracle BI alerts, known as iBots, also exists in the Oracle BI Delivers product. The privilege to use delivers is not granted to anyone in the evaluated configuration. It is out of scope of the TOE.

User applications make calls to the Web Services to obtain access to Oracle BI Presentation Services. These return HTML pages or XML datasets that can be displayed via a web browser to the user. The Web Services will be configured to use HTTPS to ensure data confidentiality generally and especially of user and password pairs submitted for authentication.

Administrative user access is also available via the BI Answers web interface. Non-administrative users are denied access to the TOE through this interface as they do not have sufficient privilege. BI Answers offers the following services for administrators:

- Present user data using charts, pivot tables, and reports.
- Save, organize, and share user data returned by requests.

- Requests created can be saved in the Oracle BI Presentation Catalog.
- Requests created can be integrated into any Oracle BI home page or dashboard, and accessed by normal users via the web services.
- Results can be enhanced through charting, result layout, and calculation also available via the web services.
- Configure Initial Access Controls on all the above presentation catalog items.

2.2.3 Oracle BI Presentation Services

Presentation Service Content

An authenticated user is provided with access to Requests. These deliver reports back in HTML format. If a user has sufficient privilege they may also send logical queries.

Requests are subject to access controls. Users will only be able to execute requests for which they are authorised. For example, a mid-level manager would not need to be granted access to a request containing summary information for an entire department.

Presentation Catalog

The presentation service content is stored and managed in the presentation catalog. Content is organized by administrators into folders that are either shared or personal. The administrator control who can change permissions on catalog objects. Object owners can always change permissions. The list of object types stored in the catalog can be found in Annex B. The web services API provides access for users to execute requests. The other object types (with the exception of folders and links) can be retrieved for processing on the client side in XML.

Managing the Presentation Catalog

Administrators are able to manage the presentation catalog overall via the web services or via a Windows server with a connection into the Presentation catalog or BI Answers. These can be used to edit, rename, set permissions for, and delete folders, filters and requests in the catalog. All other users have access to a subset of the presentation catalog determined by privilege and access control permissions, via web services calls.

2.2.4 Oracle BI Java Host

This is a security irrelevant component of the TOE that provides facilities that the Presentation Services use to produce charts, gauges and ‘.pdf’ objects that can be output as part of Reports. They are used to present the output from requests and queries to the user via the web services.

2.2.5 Oracle BI Server

This is the command centre for Oracle BIEE controlling authentication, user accountability, access to the business model, and access to the back end Oracle Database Management System that stores the physical database tables. Administrators use this to define and partition the organisational business model to give users the access to the parts of the business model required for their role.

When logical queries are submitted from Oracle Presentation Services, the BI Server translates these into SQL that is processed by the database. Results are served up to the Presentation Services as Reports. Every query that is submitted is logged in the query log, which ensures that users are accountable for their actions.

Oracle BI Repository

The BI Server stores a set of logical tables in its repository. These correspond to the physical tables in the back end database. A representation of the physical tables are imported from the Oracle Database Management System. The resulting metadata is stored in repositories and can be structured at the Presentation Services level to provide the kind of views required by the user community.

Oracle BI Administrator Tool

Administrators use the local Oracle BI Administrator tool via a Windows ODBC channel to the BI Server to perform the configuration of the following features:

- Authentication method used (Database direct or Oracle Internet Directory (OID)); and
- Where the user community in terms of user accounts and groups is sourced (i.e. in the database or in Oracle Internet Directory).

2.3 IT Environment for the TOE

This can be considered from two perspectives, the IT environment underlying the TOE and the peer to peer IT environment to the TOE.

Underlying IT Environment

Oracle Enterprise Linux (OEL) version 4 update 5 is being used as the operating system platform for the TOE. It has been evaluated to EAL4. The access controls and secure configuration are being relied upon to protect the underlying data, configuration and software integrity. As far as possible the evaluated configuration of OEL has been used in its evaluated configuration.

Oracle HTTP Server (OHS version 10.1.3) is the web server component of Oracle Application Server. It is based on the Apache 2.0 HTTP Server. Its primary function is to service requests from clients made through the HTTP protocol, although for the TOE it is being used as a proxy server, both forward and reverse. It ensures all connections to the TOE are made via HTTPS. As far as possible the evaluated configuration of OHS has been used.

Oracle Containers for Java (OC4J version 9.0.4), with the presentation services plug-in deployed within it (version 10.1.3.3.2) with Quick Fix 090406, serves to direct requests for access to the BI Presentation Services. As far as possible the evaluated configuration of OJ4J has been used. The presentation services plug-in is considered to be out of the scope of the TOE itself.

Peer to Peer IT Environment

Oracle BIEE has the capability to operate with both multi-dimensional and relational data sources. The relational data source used in the evaluated configuration is the Oracle 10g Database Management system Release 2 (10.2.0). This software has been evaluated to EAL4 and is used in its evaluated configuration. Additionally, Oracle Advanced Security (10.2.0) is used to enable encryption of data between the Database and OBIEE and vice versa.

Oracle 10g Internet Directory (10.1.4.0.1) may be used to provide authentication for the OBIEE. It has been evaluated to EAL4 and is used in its evaluated configuration.

2.4 TOE Security Architecture

Identification and Authentication

Each user is identified by a username and group information held by Oracle Internet Directory (OID) *or* on the back end Database. Each user has a password that is used to authenticate them to Oracle BIEE. Figure 2.3 below

shows the components from the security architecture involved in authentication.

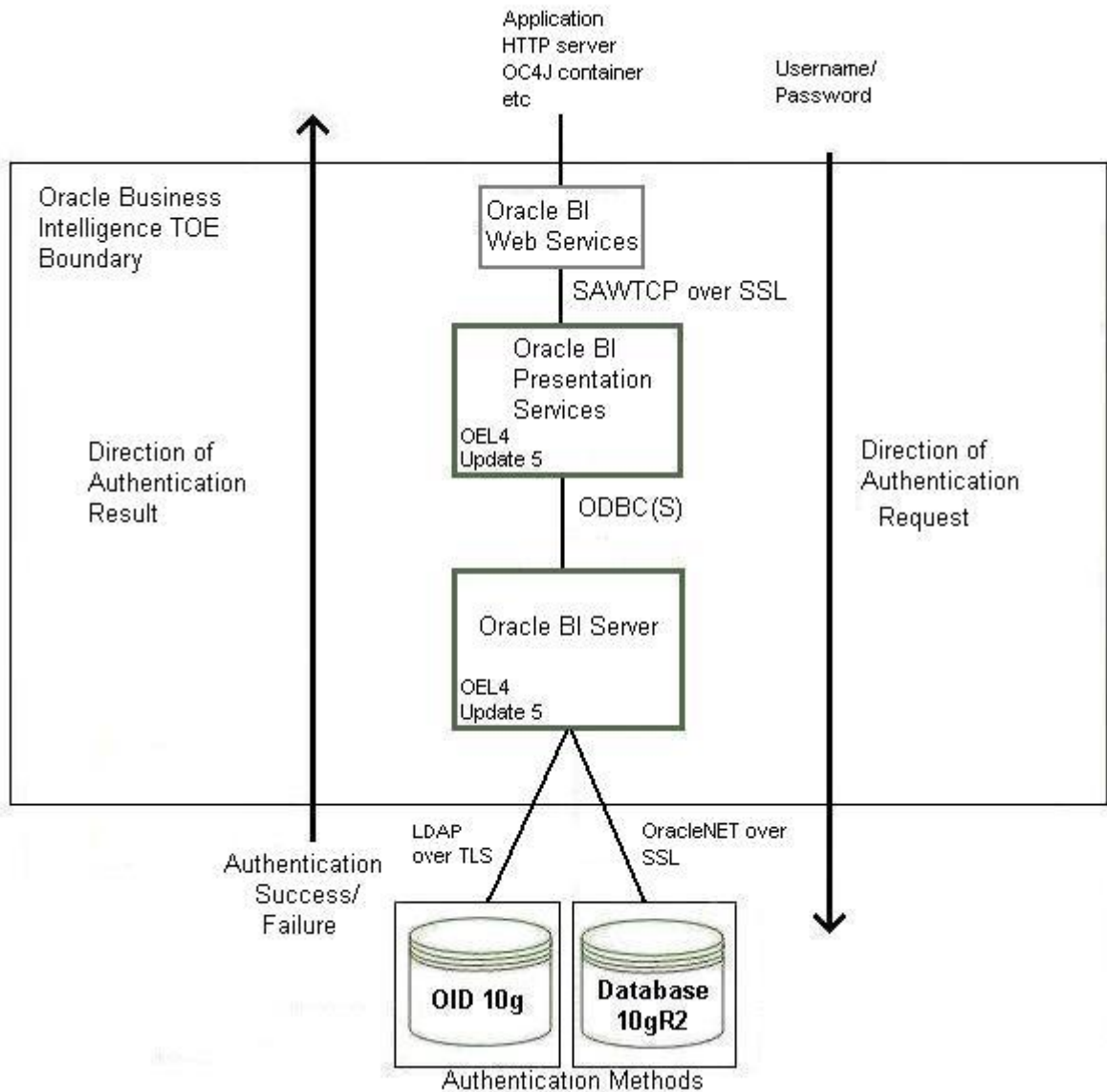


Figure 2.3: Oracle BIEE components and authentication

Every BI Server repository created has an administrator with super user access to it and all features required for its administration. Administrators can also log on locally to a BI server to administrate it. This authentication is not handed off to OID or the database. This interface is required to be physically protected so the administrator authentication is outside the scope of the evaluation.

Authentication is the process of proving that a user is who he or she claims to be. All user requests for authentication are received by the Web Services through the Presentation Services and passed to the BI Server. This in turn passes authentication through to one of two entities:

Type of authentication	Description
Database	The server submits the username and password pair directly to the database, which performs authentication and returns the result. This is then taken and used to create a user session on the TOE or provide an error message to the user. The Oracle Database authentication service provides for limits on the number of attempts, and password policies.
Oracle Internet Directory (OID)	The server hands off the authentication to OID, passing the username and password. Based on the result by OID, the user is permitted access or not. OID provides similar services to the Database in terms of protecting authentication from abuse.

Figure 2.4: Types of authentication available within Oracle BIEE.

Access Control

Every object stored by the Presentation Services has an Access Control List. These lists, often referred to as ACLs, are comprised of Access Control Items or ACIs. ACLs govern the way presentation or data objects are accessed, specifying who obtains access. The main purpose for ACLs, therefore, is to occupy a role in providing a secure environment where users who need access to data are granted it, and those who should not have access are denied it.

Oracle BIEE provides access controls at the level of the Presentation Services. Users are able to configure access to the former limited by privilege through web service calls operating on requests¹. Administrators have super user access to all objects in the TOE and total rights for configuring access control. The TOE also includes the notion of an object Owner. This user is subject to access controls, but always retains the “Change Permissions” privilege on the object. An object can have more than one owner.

¹ The result of executing a request is called a Report.

User Accountability

The auditing feature of Oracle BIEE collects and presents data pertaining to user queries and access attempts. At the most detailed level, the accounting log stores when a query was submitted and who submitted it. This also includes information about the number of rows returned and the tables accessed.

Oracle BIEE stores the accounting log in the backend database, which can then be queried by Administrators like any other data object. The level of logging is configurable. The evaluated configuration will employ maximum level logging.

Data Exchange

Oracle BIEE consists of separate physical components that pass user data and credentials to each other. HTTPS (implemented using OpenSSL version 0.9.8j) is used internally to protect this data from unauthorised access; and also externally in communication with user applications using the Web Services via the Oracle Web server. Oracle Advanced Security Option is used to encrypt communications with the back end database.

3 Security Problem Definition

This part of the ST provides the security problem definition, which defines the security problem the TOE and its operational environment is intended to address. To this end, it specifies:

- the threats that the TOE and its operational environment must counter,
- the assumptions made about the operational environment.

There are no organisation security policies defined for this TOE.

3.1 Threats

The assumed threats to TOE security, along with the threat agents which might instigate these threats, are specified below. Each threat statement identifies a means by which the TOE and its underlying system might be compromised.

These threats will be countered by:

- Technical security measures provided by the TOE, in conjunction with
- Technical security measures provided by the underlying system, and
- Non-technical operational security measures (personnel, procedural and physical measures) in the operational environment.

3.1.1 Assets requiring protection

The IT assets requiring protection consist of the data that users can access as a result of having access to Oracle Business Intelligence. The primary IT assets are:

- User data including data about products, customers, prices, contacts, activities, assets, opportunities, employees, and other elements as defined by the data owners.

The secondary assets are:

- Repository administrator login credentials.
- Configuration settings that clamp down the features of the product so that it operates in a secure manner.

- Access Control Policy data that specifies which users are permitted access to what data and features within Oracle BI.
- Audit data generated by the TOE during its operation.

3.1.2 Threat agents

The threat agents are:

- Users who are capable of making requests to access IT assets through the TOE and specifying new viewpoints to the IT assets;
- System Users who are persons authorized to use the IT environment (or system) underlying the TOE;
- Outsiders who are persons that are not authorised users of the TOE or IT environment underlying the TOE (operating system and/or database systems and/or web servers and/or network services and/or custom software);
- Operational Interrupters that cause the operation of the TOE to be interrupted as a result of failures of hardware, power supplies, storage media etc, where the source of the threat may be human (e.g. suppliers of equipment) or non-human (e.g. hardware glitches and natural disasters).

Threat agents can initiate the types of threats against the IT assets that are listed below.

3.1.3 Statement of threats²

The threats in this section are countered by technical security measures provided by the TOE, supported by technical security measures provided by the underlying system and non-technical operational security measures in the environment.

The TOE provides granulated access controls for users to corporate data and the reports available to structure and display that data. Figure 2.1 shows a user is situated at an application making access requests to the TOE via a Web Services API. The primary threat arises from one of two scenarios. First, attackers using this as their attack path to obtain unauthorised access to and

² Note for this TOE there are no Organisational Security Policies, only threats.

control of the TOE. Second, authorised users seeking to obtain access via this path to data or services for which they are not authorised.

T.DATA Unauthorized Access to Resources. A user obtains unauthorized access to data resources via the user interface to the TOE.

Note that data resource in this threat could be a data object or a feature of the TOE used to present that data to users.

T.ACCESS Unauthorized Access to Security Attributes. A user obtains unauthorized access to security attributes via the user interface to the TOE.

T.ATTACK Undetected Attack. An undetected compromise of IT assets occurs as a result of an attacker attempting to perform actions, which the individual is not authorized to perform, via the user interface to the TOE.

Note that this threat is included because, whatever countermeasures are provided to address the other threats, there is still a residual threat of a violation of the security policy occurring by attackers attempting to defeat these countermeasures (e.g. by attempting to crack a user's password).

T.TRANSIT Eavesdropping of data in transit. A user obtains unauthorised access to data resources by eavesdropping data in transit between physically separate components of the TOE; between users and the TOE; and between the TOE and its user community.

T.INTEGRITY Modification of data in transit. A user modifies data in transit between separate TOE components.

T.REPLAY Replay of data in transit. A user records data in transit between separate TOE components and then replays it to gain access to TOE features and data.

T.ABUSE.USER Abuse of Privileges. An undetected compromise of IT assets occurs as a result of a user (intentionally or otherwise) performing actions the individual is authorized to perform.

Note that this threat is included because, whatever discretionary access control countermeasures are provided to address the other threats, there is still a residual threat of a violation of the security policy occurring, or IT assets being placed at risk, as a result of actions taken by authorized users. For example, a user may grant access to a directory object they are responsible for

to another user who is able to use this information to perform a fraudulent action.

In addition, the following threats are countered by the Operating Environment:

TE.ACCESS Unauthorized Access to IT Assets. An outsider or system user obtains unauthorized access to IT assets other than via the user interface to the TOE.

Note that this threat is the environmental analogue of T.DATA and T.ACCESS.

TE.OPERATE Insecure Operation. Compromise of IT assets may occur because of improper configuration, administration, and/or operation of the composite system.

TE.CRASH Abrupt Interruptions. Abrupt interruptions to the operation of the TOE may cause security related data, such as audit data, to be lost or corrupted. Such interruptions may arise from human error or from failures of software, hardware, power supplies, or storage media.

TE.ATTACK Undetected Attack. An undetected compromise of IT assets occurs as a result of an attacker attempting to perform actions, which the individual is not authorized to perform via the user interface to the IT environment.

3.2 Assumptions

This part of the security problem definition scopes the security problem by identifying what aspects of the operational environment are taken to be axiomatic.

The TOE is dependent upon both technical IT and operational aspects of its environment.

3.2.1 TOE Assumptions

A.TOE.CONFIG The TOE is installed, configured, and managed in accordance with its evaluated configuration described in [ECG].

Note that, as stated in OE.INSTALL, [ECG] defines the evaluated configuration in detail. It states requirements for the installation and configuration of the underlying system, describes how to install the TOE from its issue media and specifies actions that must be taken by the administrator to ensure the security of the evaluated configuration. Examples of such actions

are the setting of restrictive permissions on operating system files and the generation of strong passwords and their secure communication to users.

3.2.2 Underlying System Assumptions

- A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the underlying system and the security of the information it contains who can be trusted not to abuse their privileges.
- A.PEER The other IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.
- A.PHYSICAL The security-critical parts of the TOE and the underlying system (including processing resources and network services) are located within controlled access facilities which prevent unauthorized physical access.
- A.SYS.CONFIG The underlying system (operating system and/or secure network services) is installed, configured, and managed in accordance with its secure configuration documentation.
- A.HTTPS The underlying system ensures that only appropriately encrypted communications reach the TOE from the user community and back end database.
- A.NETWORK The security-critical software of the TOE and the underlying system (including network services) are logically protected using firewall technology which prevent unauthorized network access.

4 Security Objectives

This part of the ST defines the security objectives that the TOE and its operational environment must achieve in order to fully solve the security problem defined in Section 3. It delineates the responsibilities of each in solving the security problem, by defining specific security objectives for the TOE and for the operational environment.

4.1 TOE Security Objectives

This section defines the security objectives that the TOE is expected to achieve, in order to solve its part of the security problem.

O.I&A The TOE must uniquely identify all users, and must authenticate the claimed identity before granting the user access to the system.

O.ACCESS The TOE must prevent unauthorized access to resources and security attributes protected by OBIEE.

O.AUDIT.GEN The TOE must provide the means of generating records of security relevant events in sufficient detail to help an administrator of the TOE to detect user queries that subvert the configured OBIEE security policy.

O.ADMIN The TOE must provide functionality which enables an authorised administrator to effectively manage access to the TOE and its data, and will ensure that only authorised Administrators are able to access such functionality.

O.CRYPTO The TOE must protect communications between:

- itself and the users;
- itself and its data sources; and
- its physically separate components

so that data in transit is not eavesdropped, modified or replayed.

4.2 Security Objectives for the Operational Environment

This section defines the security objectives that the operational environment is expected to achieve, in order to solve its part of the security problem. The following IT security objectives are to be satisfied by the environment in which the TOE is used.

IT Security Objectives

OE.ADMIN The underlying system must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized

Administrators can access such functionality. In particular, to enable the effective management of the TOE's audit functions the underlying operating system's functions must include the provision of reliable timestamps for use in audit records.

OE.AUDIT.GEN The underlying system must provide the means of generating records related to the security events in sufficient detail to help an administrator of the TOE to:

- a) Detect attempted authentication violations to the TOE; and
- b) Determine what connections are made to the TOE via the web service.

Note: these events are stated because they are required to support the accounting performed by the TOE and are not performed by the TOE itself. An complete account of the capability of the OEL accounting system can be found in the security target for OEL [OEL_ST].

OE.AUDIT.QUERY The underlying system database must provide tools to query the audit trail for OBIEE to enable full security auditing of the TOE.

OE.AUDIT.SIZE The underlying system database must monitor and manage the size of the audit trail so that accounting information is not lost.

OE.AUDIT.SYSTEM The underlying system must maintain a protected audit trail for OBIEE so that Administrators can use it to detect and investigate security incidents.

OE.FILES The underlying system must provide access control mechanisms by which all of the TOE related files (including executables, run-time libraries, database files, xml configuration files, export files, redo log files, control files, audit files, trace files and dump files) and TOE related database tables may be protected from unauthorized access.

OE.I&A The database or LDAP directory in the underlying system must accept credentials for an authenticated user provided by the OBIEE without requiring further authentication for a session.

OE.SEP The underlying operating system must provide the means to isolate the TOE Security Functions (TSF) and assure that the TSF components cannot be tampered with.

OE.PEER The underlying system IT components are managed such that they are under the same security policy as the TOE.

OE.SSL The underlying system provides SSL where necessary to ensure that communications with the TOE are encrypted.

OE.NETWORK The underlying system provides firewall technology where necessary to ensure that direct network attack on the TOE is prevented.

OE.PORTS The underlying system is locked down such that the only necessary logical access points to its constituent components are exposed.

Non-IT Security Objectives

The following non-IT security objectives are to be satisfied by procedural and other measures taken within the operational environment.

OE.ACCOUNT Administrators of the TOE will ensure that the TOE is configured such that only the approved group of users for which the system was accredited may access the system.

OE.AUDITLOG Administrators must ensure that audit facilities are used and managed effectively. These procedures shall apply to the TOE's audit trail and the audit trail for the underlying system. In particular:

- a) Appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space;
- b) Audit logs must be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future;
- c) The system clocks must be protected from unauthorized modification and checked for time drift (so that the integrity of audit timestamps is not compromised).

OE.AUTHDATA Those responsible for the TOE must ensure that the authentication data for each user account for the TOE and for each user account for the underlying system is held securely and not disclosed to persons not authorized to use that account. In particular:

- a) The media on which the authentication data for the underlying operating system is stored shall not be physically removable from the underlying platform by unauthorized users;
- b) Users shall not disclose their passwords to other individuals;
- c) Passwords generated by the system administrator shall be distributed in a secure manner.

OE.INSTALL Those responsible for the TOE must ensure that:

- a) The TOE is delivered, installed, managed and operated in accordance with the operational documentation of the TOE, and in particular its evaluated configuration as defined in [ECG], and
- b) The underlying system is installed and operated in accordance with its operational documentation. If the system components are certified under the Common Criteria they should be installed and operated in accordance with the appropriate certification documentation.

Note that [ECG] defines the evaluated configuration of the TOE in detail. It states requirements for the installation and configuration of the underlying system, describes how to install the TOE from its issue media and specifies actions that must be taken by the administrator to ensure the security of the evaluated configuration. Such specified actions may emphasise items already

documented in the TOE's administrator guidance documentation or may provide additional instructions to avoid potential security problems that relate to the evaluated configuration.

OE.MEDIA Those responsible for the TOE must ensure that the confidentiality, integrity and availability of IT assets held on storage media is adequately protected. In particular:

- a) The on-line and off-line storage media on which IT assets and security related data (such as operating system backups, database backups and transaction logs, and audit trails) must not be physically removable from the underlying platform by unauthorized users;
- b) The on-line and off-line storage media must be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related-data;
- c) The media on which TOE-related files (including database files, export files, redo log files, control files, trace files and dump files) have been stored shall be purged prior to being re-used for any non-directory purpose.

OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE and the underlying system that are critical to the security policy are protected from physical attack.

OE.RECOVERY Those responsible for the TOE must ensure that procedures are in place to ensure that, after system failure or other discontinuity, recovery without security compromise is obtained.

OE.TRUST Those responsible for the TOE must ensure that only users, who can be trusted to perform administrative duties with integrity, have privileges which allow them to:

- a) set or alter the configuration directives affecting audit record generation by the TOE;
- b) set or alter the configuration of the audit trail maintenance system;
- c) modify the contents of the audit trail;
- d) create any user account or modify any security attributes of users other than themselves;
- e) set or alter security attributes that affect the ability of users other than themselves to access resources; or
- f) set administrative permissions on files.

Note that one user would not normally simultaneously hold all of these privileges. Thus an audit administrator would normally be given the privileges for items a), b) and c) while a system administrator would be given the privileges for d) e) and f).

The rationale tables in chapter 6, section 1 illustrate how each of the above objectives counter a threat, or map to a secure usage assumption.

5 Security Requirements

This part of the ST defines the security requirements that the TOE must meet in order to achieve the corresponding security objectives defined in Section 4. Requirements for the TOE are divided into Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs). The CC requires that these be constructed, where possible, using security functional and assurance components defined, respectively, in [CC2] and [CC3].

This part of the ST also meets the requirements for a TOE Summary Specification by interspersing the description of how the TOE provides the SFRs.

The text for completed operations which have been applied to the SFRs is as follows:

Assignment: indicated with bold text

Selection: indicated with underlined text

Refinement: additions indicated with bold text and italics, deletions indicated with strike-through bold text and italics

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g. FCS_CKM.1.1a)

The explicitly stated requirements claimed in this ST are denoted by the “.X” extension in the unique short name for the explicit security requirement (e.g. FAU_GEN.X).

5.1 Security Functional Requirements

5.1.1 Class FAU: Security Audit

5.1.1.1 FAU_GEN.2: User identity association

FAU_GEN.2.1 ***For audit events resulting from the queries and access attempts of identified users***, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

TOE Summary Specification: FAU_GEN.2

The data submitted with a query by the TOE on behalf of a user includes references to a session id bound unambiguously with the user. In this sense, the TOE submits queries on behalf of a user. This ensures that every query is associated with the identified user who submits it.

5.1.1.2 FAU_GEN.X: Audit data generation

FAU_GEN.X.1a The TSF shall be able to generate an audit record for every logical query executed by the TOE.

FAU_GEN.X.2a The TSF shall record within each audit record at least the following information:

- a) Date and time,
- b) Username,
- c) Number of database queries submitted for the logical query,
- d) The Logical SQL text submitted,
- e) The business model accessed,
- f) The outcome whether success or failure,
- g) The number of rows returned.

TOE Summary Specification: FAU_GEN.X.1a and 2a

The Oracle BI Presentation Server operates by only allowing users to “see” objects to which they have explicit access. In this way, users are unable to make attempts to access parts of the data model for which they have no authorisation. This limits the attack surface on the server considerably. Any attack will arise from a user guessing the identity of data they wish to access, or having independent knowledge of its presence and path. The functionality required by FAU_GEN.Xa provides the optional capability for the Oracle BI Server to store information about every logical query executed so the residual possibility of injected malformed queries to the server can be detected.

Item (f) returns “0” if the query was successful, and one of the following if not:

- 1 indicates a timeout;
- 2 indicates a row limit violation; and
- 3 indicates an Unknown error.

The audit records (called “usage tracking log” in Oracle BI terms) are stored in the back-end Oracle 10g database.

FAU_GEN.X.1b The TSF shall be able to generate an audit record for every *Presentation Services object access failure by a user*.

FAU_GEN.X.2b The TSF shall record within each audit record at least the following information:

- a) *Date and time of access attempt,*
- b) *Object to which access was denied and*
- c) *Username attempting access.*

TOE Summary Specification: FAU_GEN.X.1b and 2b

This SFR complements FAU_GEN.Xa at the presentation server. It provides a mechanism to identify when users fail to read Presentation Services objects by explicitly logging every object access failure by username, date, time and object name.

The audit records are stored in flat file within the OEL audit subsystem.

5.1.2 Class FCS: Cryptographic support

5.1.2.1 FCS_CKM.1: Cryptographic key generation

FCS_CKM.1.1a The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **TDEA** and specified cryptographic key sizes **168 bits** that meet the following: **no external standard used**.

FCS_CKM.1.1b The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **1024 and 2048 bits** that meet the following: **no external standard used**.

TOE Summary Specification: FCS_CKM.1

The TOE generates 168bit keys for use in TDEA cryptographic operations. It generates 1024 or 2048 bit keys for RSA.

Key generation is provided by OpenSSL where connections are initiated from the TOE.

5.1.2.2 FCS_CKM.2: Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **Asymmetric Key Wrapping using RSA** that meets the following: **no external standard used**.

TOE Summary Specification: FCS_CKM.2

The TOE uses RSA Key wrapping to securely distribute keys between the Presentation Server and BI server; and between the BI server internally; between client and Presentation Server; and between BI server and Oracle web server. For more information see FPT_ITT.1 and FPT_ITC.1.

5.1.2.3 FCS_CKM.4: Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **OpenSSL Overwrite of all plaintext cryptographic keys and other critical security parameters** that meets the following: **none**.

TOE Summary Specification: FCS_CKM.4

The TOE ensures that all keys are overwritten with the value of zero at the end of their lifetime.

5.1.2.4 FCS_COP.1: Cryptographic operation

FCS_COP.1.1a The TSF shall perform **data encryption and decryption operations** in accordance with a specified **OpenSSL TDEA** cryptographic algorithm and **a 168 bit** cryptographic key sizes that meets the following: **no external standard used**.

FCS_COP.1.1b The TSF shall perform *data encrypt and decrypt operations for key wrapping* in accordance with a specified **OpenSSL RSA** cryptographic algorithm and **2048 bit** cryptographic key sizes that meets the following: **no external standard used**.

TOE Summary Specification: FCS_COP.1

The TOE implements a TDEA in OpenSSL to provide encrypt and decrypt services within the TOE using 168 bit keys. The use to which this algorithm is put is defined under FPT_ITC.1 and FPT_ITT.1.

RSA is also implemented in OpenSSL to provide encrypt and decrypt services within the TOE for key wrapping. A 2048 bit key size is used. See FCS_CKM.1.1b and FCS_CKM.2.1b.

5.1.3 Class FDP: User data protection

Please note that each rule in each iteration of FDP_ACF.1.2 is checked. Conflicts are resolved by the rules in FDP_ACF.1.3 and FDP_ACF.1.4.

5.1.3.1 Presentation Objects Access Policy

FDP_ACC.1.1a The TSF shall enforce the **Presentation Objects Access policy** on:

- **all users and their associated group memberships;**
- **the following object types: Requests, Filters, Folders, Links and the objects listed in Annex B; and**
- **all operations between them.**

FDP_ACF.1.1a The TSF shall enforce the **Presentation Objects Access policy** to objects based on the following:

- a) **the authorized user identity and associated group membership(s);**
- b) **access permissions associated with Requests, Filters, Folders, Links and the objects listed in Annex B;**
- c) **object ownership; and**
- d) **presentation object identity.**

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among **users** and **presentation objects** is allowed:

- a) **if the user requesting access is denied access to any of the presentation objects queried, then access is denied;**
- b) **if the user requesting access has access to the presentation object for the mode requested then permit access;**
- c) **if all group memberships of the user requesting access are denied access to the presentation object requested, then access is denied;**
- d) **if any group membership for the user requesting access has access to the presentation object for the mode requested then permit access.**

FDP_ACF.1.3a The TSF shall explicitly authorise access of subjects to objects based on the following additional rule:

- **if the user is the owner of the presentation object they are permitted to change the permissions of the object;**
- **if the group membership permissions deny access but the user has explicit access.**

FDP_ACF.1.4a The TSF shall explicitly deny access of subjects to objects based on the following additional rule:

- **if the group membership permissions allow presentation object access but the user is explicitly denied access.**

TOE Summary Specification: FDP_ACC.1.1a, FDP_ACF.1.1a - FDP_ACF.1.4a

OBI Presentation service objects³ are:

- Requests;⁴
- Filters;
- Folders; and
- Links.

The TOE allows two modes of access to presentation service data objects: explicitly – where the user is granted access specifically in accordance with the ACL of the data object; and implicitly – where the user is granted access through their membership of a group assigned access in the ACL of the data object. Explicit permissions take precedence over implicit permissions.

Groups can be organised hierarchically, for example:

Everyone – the group of which every user is a member;

Generation Group1 – permission list for each object; and generation group2;

Generation Group2 – permission list for each object; and generation groupN;

...

Generation GroupN – permission list).

Any user who was a member of Generation Group 1, would also pick up the permissions in the group hierarchy up to groupN. Where the permissions conflict the least restrictive has precedence. The only exception to this is “deny”, which has precedence over every other permission.

See Annex A for an example.

The following permissions in ACLs are supported on OBI Presentation Services objects through the web services:

- No Access: permission is explicitly denied. This takes precedence over any other permissions
- Full Control: permits a user to read, execute, write, delete, set permissions, and set ownership

³ There are many other object types stored in the Presentation Catalog. However these are protected from normal user access by the ACL. Mostly, these are object types created by products that are not in the scope of the TOE (e.g. Interactive Dashboards, Delivers, etc). A complete list is provided at Annex B.

⁴ A Request is the item stored in the Presentation Catalog and has ACLs. When a request is executed it returns a Report. Sometimes the TOE user documentation uses these terms interchangeably.

on the object.

- Read: permits a user to view the content of a data object only; no changes are permitted.
- Execute: permits a user to execute an object.
- Write: permits a user to write to an object, for example to modify its content.
- Delete: permits a user to delete the object.
- Change Permissions: permits a user to change the permissions on the presentation services object.
- Set Ownership: permits a user to set ownership for the object.

Where a user is granted access, but not full control, the permissions can be compounded (e.g. a user is granted Read and Execute for RequestA). The TOE shall allow access to an Oracle BI Presentation services object where the user is explicitly or implicitly authorised to in the ACL to have it. Object owners always have “Change Permissions” access.

5.1.3.2 Presentation Services Privilege Access Policy

FDP_ACC.1.1b The TSF shall enforce the **Presentation Services Privilege Access policy** on:

- **all users and their associated group memberships;**
- **the privileges listed under FIA_ATD.1.1(c); and**
- **the Presentation Services functions to which the privileges apply.**

FDP_ACF.1.1b The TSF shall enforce the **Presentation Services Privilege Access policy** to **functions** based on the following:

- a) **the authorized user identity and associated group membership(s);**
- b) **privileges associated with each function; and**
- c) **the functions to which the privileges grant or deny a user access.**

FDP_ACF.1.2b The TSF shall enforce the following rules to determine if an operation among **users** and **functions** is allowed based on **privilege assignment**:

- a) **if the requesting user is denied access to the presentation function by privilege then deny execution;**
- b) **if the requesting user is granted access to the presentation function by privilege then grant execution;**
- c) **if all group memberships of the user requesting access are denied access to the presentation function by privilege, then deny execution;**

- d) if any group membership for the user requesting access has execution privilege to the presentation function then grant execution.**

FDP_ACF.1.3b The TSF shall explicitly authorise access of subjects to objects based on the following additional rule:

- **if the group membership permissions deny presentation function execution by privilege but the user has explicit access, then grant execution.**

FDP_ACF.1.4b The TSF shall explicitly deny access of subjects to objects based on the following additional rule:

- **if the group membership permissions allow presentation function execution by privilege but the user is explicitly denied execution privilege, then deny execution.**

TOE Summary Specification: FDP_ACC.1.1b, FDP_ACF.1.1b - FDP_ACF.1.4b

OBI Presentation service privileges are defined in FIA_ATD.1.1(c).

The TOE allows two modes of access to presentation service privileges: explicitly – where the user is granted access specifically by privilege in the ACL of the function; and implicitly – where the user is permitted execution through their membership of a group assigned privilege in the ACL of the function. Explicit permissions take precedence over implicit permissions.

Groups can be organised hierarchically:

- Everyone – the group of which every user is a member;
- Generation Group1 – privilege list; + generation group2;
- Generation Group2 – privilege list; + generation groupN;
- ...
- Generation GroupN – privilege list).

Any user who was a member of Generation Group 1, would also pick up the privileges of all the groups up to groupN. Where the privileges conflict a “deny” has precedence.

See Annex A for an example.

The following permissions in ACLs are supported on OBI Presentation Services functions for each user and group:

- Grant privilege to execute and
- Deny privilege to execute.

The TOE shall allow the execution, in principle, of an Oracle BI Presentation services function where the user is explicitly or implicitly has privilege in the ACL. When this privilege check is complete the objects involved are checked (cf. FDP_ACC.1a and FDP_ACF.1a). Actual execution of the function is only permitted where the user has privilege *and* the required access permissions.

5.1.4 Class FIA: Identification and authentication

5.1.4.1 FIA_ATD.1: User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- a) Username,
- b) Group membership(s),

c) Any of the following Oracle Presentation services privileges⁵ as applicable:

- Access to Dashboards;
- Access to Answers;
- Access to Delivers;
- Access to Briefing Books;
- Access to Disconnected Analytics;
- Access to Administration;
- Access to Metadata Dictionary;
- Access to Oracle BI Publisher for Enterprise;
- Access to Oracle BI for Microsoft Office;
- Presentation Catalog - Change Permissions;
- Presentation Catalog - Toggle Maintenance mode;
- Manage sessions;
- Manage Dashboards;
- See sessions IDs;
- Issue SQL directly;
- View System Information;
- Manage Privileges;
- Set Ownership of Catalog Objects;
- Access SOAP.

TOE Summary Specification: FIA_ATD.1

System-defined Presentation Services groups are pre-configured and required, these are:

- Everyone: all users belong to the everyone group.
- OBI Presentation Services Administrators: the default member of this group is the OBI Presentation Services Administrator; and it is used to designate who has the privilege to administrate OBI Presentation Services.
- OBI Server Administrator: the default member of this group is the OBI Server Administrator; and it is used to designate who has the privilege to administrate each repository on the OBI server. A new administrator in this group is created for each new repository is created.

The TOE shall allow the Presentation services privileges to be assigned to Administrators, users and groups. The privilege list is included in the SFR.

5.1.4.2 FIA_UAU.2: User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated, ***either implicitly or explicitly***, before allowing any other TSF-mediated actions on behalf of that user.

⁵ all OBI product privileges listed exist in the TOE but not all are necessarily applicable in the TOE Scope. The full list can be found in [AG_BIPS, pg154 - 161]

5.1.4.3 FIA_UID.2: User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

TOE Summary Specification: FIA_UAU.2 and 7, and FIA_UID.2

The TOE requires a valid username and password pair before granting access to any of its services. In the explicit case, a user is authenticated by submission of a valid username and password. In the implicit case, a user session is initiated at the request of an already authenticated administrator. It requires user identification only. Only authenticated administrators can successfully initiate user sessions in this way. Within the TOE documentation this method of user identification with implicit authentication is called 'impersonation'.

The TOE accepts the username and password from a user via a web services API.

Password entry is outside the scope of the TOE. It will be provided by a user application that uses the web services to submit username and password pairs to the TOE for authentication. This data is protected during submission using SSL in HTTPS. The TOE then hands off the authentication check to LDAP or the backend database as configured. Although, the authentication check is handed off, the TOE takes responsibility for acting upon the result of the authentication to permit or deny access. An error message is returned via the web services as applicable.

5.1.4.4 FIA_USB.1: User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- a) **The user identity which is associated with auditable events.**
- b) **The user identity used to enforce the OBI object access control policy.**
- c) **The group identity used to enforce the OBI object access control policy.**
- d) **The privilege(s) assigned to a user.**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- a) **Upon successful identification and authentication, the login username shall be that specified in the user entry for the user that has authenticated successfully, or in the case of administrator user impersonation, that has been identified by a successfully authenticated administrator.**
- b) **Upon successful identification and authentication, the group memberships shall be those specified in the group memberships for the user, or impersonated user entry.**
- c) **Upon successful identification and authentication, the user privileges shall be those specified in the privileges for the user, or impersonated user entry.**

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **none specified.**

TOE Summary Specification: FIA_USB.1

No further explanation required.

5.1.5 Class FMT: Security management

5.1.5.1 FMT_MOF.1: Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to disable **or** enable the functions **that activate authentication methods** to **Administrators**.

TOE Summary Specification: FMT_MOF.1

See the TOE Summary Specification entry for section 5.1.5.5.
--

5.1.5.2 FMT_MSA.1: Management of security attributes

FMT_MSA.1.1a The TSF shall enforce the **Presentation Services Privilege Access Policy and Presentation Object Access Policy** to restrict the ability to modify the **User and Group Access Control List** security attributes to **Administrators, Object Owners and those Users who are permitted Full Control and Change Permissions access to the object respectively.**

TOE Summary Specification: FMT_MSA.1a
--

No further explanation required.

FMT_MSA.1.1b The TSF shall enforce the **Presentation Services Privilege Access Policy** to restrict the ability to modify the **Presentation Services Privilege Access Control List** security attributes to **Administrators and those Users who have the “Manage Privileges” privilege.**

TOE Summary Specification: FMT_MSA.1b
--

No further explanation required.

5.1.5.3 FMT_MSA.3: Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Presentation Object Access Policy** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall **not** allow the **specification of** alternative initial values to override the default values when an object or information is created.

TOE Summary Specification: FMT_MSA.3

No further explanation required.

5.1.5.4 FMT_MTD.1: Management of TSF data

FMT_MTD.1.1a The TSF shall restrict the ability to set up and modify the **overall access control policy on the Oracle BI Presentation Services that control user access to the following presentation object types to Administrators: requests, filters, links, folders, MetadataDocs, KeyValueMaps, Privileges, SecurityVersions, AccountIndexes, AccountDatas, SqlNodeCaches, GUIDStates and Replications.**

FMT_MTD.1.1b The TSF shall restrict the **overall control** to modify ~~the~~ **which users and groups have which privilege on the presentation Services to Administrators.**

5.1.5.5 FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- a) **Manage which type of authentication is enabled: Database or LDAP authentication.**
- b) **Manage permissions on the Oracle BI Presentation Services relating to user access to the following types of presentation object types: requests and filters.**
- c) **Manage privileges on the Oracle BI Presentation Services.**

TOE Summary Specification: FMT_MOF.1, FMT_MTD.1 and FMT_SMF.1

The TOE only permits Administrators to configure which authentication method is active within the TOE. This management is only possible via the Admin tool user interface connected to the BI Server. The authentication methods are: Database or OID (LDAP). When a user is submitted for authentication via the web services, the TOE hands over verification of the received username and password to the appropriate module. On reply, the TOE allows or denies authentication.

Only suitably privileged users on Oracle BI Presentation Services are permitted to manage overall access to TOE data objects. This management is possible via the BI Answers and web services user interfaces to the Presentation Services. Authentication prevents access to non-privileged users..

5.1.5.6 FMT_SMR.1: Security Roles

FMT_SMR.1.1 The TSF shall maintain ~~the~~ **administrator** roles *for Presentation Services and Business Intelligence Servers.*

TOE Summary Specification: FMT_SMR.1

No further explanation required.

5.1.6 Class FPT: Protection of the TSF

5.1.6.1 FPT_ITC.1: Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to *the Oracle web server* from unauthorised disclosure **and modification** during transmission.

TOE Summary Specification: FPT_ITC.1.1

The TOE encrypts all communication sent to the Oracle web server using SAWTCP over SSL. The TOE decrypts any encrypted communication sent back.

SSL is configured to use TDEA as specified in FCS_COP.1 with mutual authentication.

5.1.6.2 FPT_ITT.1: Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure **and** modification when it is transmitted between separate parts of the TOE.

TOE Summary Specification: FPT_ITT.1

The TOE encrypts all communication sent between the Oracle BI Presentation Services and Oracle BI Server using SSL and transmits it using the ODBC(S) protocol.

SSL is configured to use TDEA as specified in FCS_COP.1 with mutual authentication and integrity checking.

5.1.6.3 FPT_TRC.X: Internal Repository consistency

FPT_TRC.X.1 The TSF shall ensure that **Repository data** is consistent when replicated between parts of the TOE.

FPT_TRC.X.2 When parts of the TOE containing replicated **Repository data** are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for **the following**:

- **authentication to the TOE**
- **access to data on the Presentation Services and Oracle BI Server.**

TOE Summary Specification: FPT_TRC.X

Note: in order to maintain the synchronisation between the primary and secondary TOE servers in its clustered configuration, the secondary TOE server services need to be manually stopped and then started to activate synchronisation. This process should be performed regularly on a schedule defined by the rate of change in the repository and at the discretion of the TOE administrator.

No further explanation required.

5.1.6.4 FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The TSF shall be able to **read** reliable time stamps **from the operating system on which it is hosted**.

TOE Summary Specification: FPT_STM.1

The TOE reads the time from the trusted Operating System on which it is hosted.

5.2 Security Assurance Requirements

The target evaluation assurance level for the product is EAL3 [CC3]. No augmented assurance requirements are included.

6 ST Rationale

This section provides the rationale for the choice of security objectives, security requirements, and IT security functions and assurance measures, demonstrating that they are necessary and sufficient to meet the security problem as defined in Section 3. This comprises the following parts:

- the security objectives rationale, demonstrating the suitability of the security objectives to solve the defined security problem;
- the security requirements rationale, demonstrating the suitability of the security requirements to achieve the TOE security objectives.

6.1 Security Objectives Rationale

The security objectives rationale demonstrates that, if all the security objectives stated in Section 4 are achieved, the security problem as defined in Section 3 is solved: in other words, all threats are countered, all OSPs are enforced, and all assumptions are upheld.

6.1.1 Suitability to counter the threats

This section demonstrates that the TOE security objectives, in conjunction with the security objectives for the environment, are suitable to counter each of the threats.

Threat	Objective	Justification
T.DATA	O.I&A	Prevents unauthorised users from accessing the TOE.
	O.ACCESS	Prevents unauthorised access to security attributes that protect and resources that store TOE assets.
	OE.ACCOUNT	Ensures that only an approved group of users have user accounts on the underlying system.
	OE.I&A	Supporting IT environment objective provides single sign on in a way that protects access to data.
T.ACCESS	O.ACCESS	Prevents unauthorised access to security attributes that protect the TOE assets.
	O.I&A	Prevents unauthorised users from accessing the TOE.

Threat	Objective	Justification
	OE.I&A	Supporting IT environment objective provides single sign on in a way that protects access to data.
T.ATTACK	O.AUDIT.GEN	Provides user accountability by storing information about security events pertinent to attack detection.
	OE.AUDITLOG	Ensures the audit trail is managed effectively.
	OE.AUDIT.SYSTEM	Ensures the provision of a protected audit trail for the TOE.
T.TRANSIT	O.CRYPTO	Protects TSF data in transit from unauthorised disclosure.
	OE.SSL	Protects user data in transit to the TOE from products in the underlying system from unauthorised disclosure.
T.REPLAY	O.CRYPTO	Protects the TSF from replay attack.
T.INTEGRITY	O.CRYPTO	Protects TSF data in transit from unauthorised modification.
	OE.SSL	Protects user data in transit to the TOE from products in the underlying system from unauthorised modification.
T.ABUSE.USER	O.AUDIT.GEN	Provides user accountability by storing information about security events pertinent to detecting abusive users.
TE.ACCESS	OE.ACCOUNT	Ensures only an approved group of users have access to the underlying system.
	OE.AUTHDATA	Ensures that authentication data is secure so that it can not be used to gain unauthorised access to the underlying system.
	OE.FILES	Provides the means of securing authentication related files in the underlying system so that its authentication mechanisms remain secure.
	OE.NETWORK	Ensures that the TOE network is protected against external intrusion.
	OE.PORTS	Ensures that the underlying system is locked down such that only necessary access points are exposed.
TE.OPERATE	OE.INSTALL	Ensures that the underlying system is securely configured.

Threat	Objective	Justification
	OE.PEER	Ensures that the underlying system is managed such that it supports the security policy of the TOE.
TE.ATTACK	OE.AUDIT.GEN	Provides a means of holding users accountable for their actions on the underlying system.
	OE.AUDIT.SIZE	Ensures that issues surrounding the management of the size of the audit trail does not cause audit records to be lost in the underlying system.
	OE.AUDIT.SYSTEM	Ensures the provision of a protected audit trail for the TOE.
	OE.FILES	Ensures the files in the underlying system that hold the audit trail can be protected.
	OE.MEDIA	Ensures that when the audit trail is written to removeable media that it is adequately protected.
TE.CRASH	OE.RECOVERY	Ensures that administrators know how to achieve physical recovery of the underlying system without security compromise.
ALL	O.ADMIN	Counters every threat by providing functions for a restricted group of Administrators to manage the TOE and its security functions, e.g. audit, access control, authentication, crypto functions, etc.
	OE.ADMIN	Provides the functions needed by an administrator in the underlying system to manage security without compromise.
	OE.PHYSICAL	Ensures that the physical parts of the underlying system and TOE that are critical to security are protected from physical attack.
	OE.SEP	Ensures that the TOE and its underlying system has protected memory space for its operation.
	OE.TRUST	Ensures that only those who can be trusted have administrative privilege to configure the TOE.

Table 6.1: Suitability of Objectives to Counter Threats

6.1.2 Suitability to uphold the assumptions

This section demonstrates that the security objectives for the operational environment are suitable to uphold each of the assumptions.

Assumption	Objective	Justification
A.MANAGE	OE.TRUST	Self evident
A.PEER	OE.PEER	Self evident
A.PHYSICAL	OE.PHYSICAL	Self evident
A.SYS.CONFIG	OE.ADMIN	Self evident
	OE.INSTALL	Self evident
A.TOE.CONFIG	OE.ADMIN	Underlying system enables only Administrators to install and configure the TOE.
	OE.INSTALL	Self evident
	OE.TRUST	Self evident
	OE.ACCOUNT	Self evident
	OE.AUDITLOG	Self evident
A.HTTPS	OE.AUTHDATA	Self evident
	OE.PEER	Underlying system is configured to use SSL when communicating between its separate components in the same way as the TOE itself. This ensures that only encrypted requests for access reach the TOE.
A.NETWORK	OE.NETWORK	Self evident
	OE.PORTS	Self evident

Table 6.2: Suitability of Objectives to Uphold Assumptions

6.2 Security Requirements Rationale

This section demonstrates that, if the TOE meets all the stated SFRs, then all TOE security objectives will be achieved.

6.2.1 Suitability to achieve the security objectives

This section demonstrates that the SFRs are suitable to achieve the TOE security objectives.

TOE objective	SFR(s)	Justification
O.I&A	FIA_ATD.1	Identifies the security attributes stored for each user.

TOE objective	SFR(s)	Justification
	FIA_UAU.2	Requires successful authentication before allowing TOE access to users.
	FIA_UID.2	Requires successful authentication before allowing TOE access to users.
	FMT_MOF.1	Only Administrators can configure the type of authentication relied upon by the TOE.
	FPT_ITC.1	Protects security related user session data from interception after successful authentication.
	FDP_ACC.1a FDP_ACF.1a	Protects user and group access to Database resources available via the TOE.
O.ACCESS	FIA_ATD.1	Provides a hierarchy of privileges that allow users to access the separate user and administrative functions of the TOE.
	FIA_USB.1	Ensures that user security attributes are associated with the processes that operate on their behalf. These attributes are the basis of the access control decisions in FDP_ACC and FDP_ACF families.
	FMT_MSA.3a – b	Enforces restrictive default access permissions when objects are created under the access control policies.
	FMT_MTD.1	Ensures that certain security oversight functions are limited to Administrators only.
	FPT_TRC.X	Ensures the Repository that holds all the meta data for back end database access are consistently replicated across the TOE.
	FAU_GEN.Xa FAU_GEN.Xb	Ensures that an audit record is generated for each query submitted by a user and that the relevant information is captured for the detection of security breaches.
O.AUDIT.GEN	FAU_GEN.2	Ensures that users are held accountable for the queries that they submit.
	FPT_STM.1	Provides a trusted source of time for the holding users accountable.
	FMT_MOF.1	Enables Administrators to manage authentication.

TOE objective	SFR(s)	Justification
O.ADMIN	FMT_MSA.1a – b	Identifies who can set the security attributes for each applicable access control policy.
	FMT_MTD.1a – c	Enables Administrators to have overall responsibilities for TOE access control and privilege assignment.
	FMT_SMF.1	Identifies all administration functions.
	FMT_SMR.1	Identifies the administrator role maintained by the TOE.
	FCS_CKM.1	Key generation for the algorithms used to encrypt communications.
O.CRYPTO	FCS_CKM.2	Secure key distribution so that an encrypted communications session can be established.
	FCS_CKM.4	Secure key destruction after communications have completed.
	FCS_COP.1	Identifies the data encryption and decryption services used.
	FPT_ITC.1	Identifies communications sessions from the TOE to external IT systems that require encryption.
	FPT_TRC.X	Ensures that repository data is consistent when replicated between physically separate parts of the TOE.
	FPT_ITT.1	Identifies internal communications sessions to be encrypted.

Table 6.3: Suitability of SFRs to Achieve TOE Security Objectives

6.2.2 Dependency analysis

Table 6.4 below provides the dependency analysis amongst the SFRs. This supports the rationale for the suitability of the SFRs to achieve the TOE security objectives, by demonstrating that there are no unresolved dependencies amongst the SFRs that would result in a TOE security objective not being achieved.

The assumptions apply:

- No justification is included where all the dependencies from [CC2] are included in the TOE. [CC2] dependencies are highlighted **bold**.
- Dependencies for iterations are only explicitly identified where they are missing for an iteration, otherwise, the reader can be sure that each iteration has a corresponding iteration for the SFR on which it is

dependent (for example, FCS_CKM.1a and FCS_CKM.1b have corresponding SFRs in FCS_COP.1a and FCS_COP.1b, etc).

SFR	Dependency	Justification
Security Audit		
FAU_GEN.X	FPT_STM.1	Note: this relies upon FPT_STM.1 in [OEL_ST, 5.1.6.4]
FAU_GEN.2	FAU_GEN.1	
	FIA_UID.1	
Cryptographic Support		
FCS_CKM.1	FCS_COP.1	
	FCS_CKM.4	
FCS_CKM.2	FCS_CKM.1	
	FCS_CKM.4	
FCS_CKM.4	FCS_CKM.1	
FCS_COP.1	FCS_CKM.1	
	FCS_CKM.4	
User Data Protection		
FDP_ACC.1a	FDP_ACF.1a	
FDP_ACF.1a	FDP_ACC.1a	
	FMT_MSA.3	
FDP_ACC.1b	FDP_ACF.1b	
FDP_ACF.1b	FDP_ACC.1b	
	FMT_MSA.3	This is not applicable to the privilege policy as new functions and privileges can not be created. They are considered initially secure when configured in accordance with [ECG].
Identification and Authentication		
FIA_ATD.1	None	N/A
FIA_UAU.1	FIA_UID.1	
FIA_UID.1	None	N/A
FIA_USB.1	FIA_ATD.1	
Security Management		
FMT_MOF.1	FMT_SMF.1	
	FMT_SMR.1	
FMT_MSA.1	FDP_ACC.1	
	FMT_SMF.1	
	FMT_SMR.1	
FMT_MSA.3	FMT_MSA.1	
	FMT_SMR.1	

SFR	Dependency	Justification
FMT_MTD.1	FMT_SMF.1	
	FMT_SMR.1	
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	
Protection of the TSF		
FPT_ITC.1	None	N/A
FPT_ITT.1	None	N/A
FPT_TRC.X	FPT_ITT.1	
FPT_STM.1	None	N/A

Table 6.4: Security Requirement Dependency Analysis

6.2.3 Bypass Protection

Bypass attacks are protected against within the TOE via the following SFR classes:

- FCS and FPT: these prevents bypassing of authentication by providing encryption services that secure the TOE against an attacker intercepting authentication credentials.
- FDP: this prevents bypassing of the security policy governing data access.
- FIA: this ensures user accountability on the TOE.

Additionally, the OEL file system protects the underlying files, databases, and data from tampering that might otherwise effect a bypass attack. The dependency analysis in section 6.2.2 demonstrates how all the SFRs in the TOE work together to achieve its security objectives.

6.2.4 Assurance Level Suitability

The target assurance level is EAL3. This is appropriate for the TOE because it is designed for use in environments where this level of assurance suitably reduces the security risk to the assets under protection by the TOE. This is attested to by the fact that EAL3 exceeds EAL2, which is the minimum assurance level set by [BR-DBMS]: the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments. Although, the TOE is not a database management system, it acts as a protective wrapper and access point to database assets. It is therefore compelling to find that the TOE measures up in that context.

7 Extended Components Definition

7.1.1 Class FAU: Security Audit

7.1.1.1 FAU_GEN.X:

Hierarchical to: No other components

Dependencies: FAU_GEN.2

This SFR is based upon FAU_GEN.1.

FAU_GEN.X.1a The TSF shall be able to generate an audit record for every [Assignment: *type of security event*] executed by the TOE.

FAU_GEN.X.2a The TSF shall record within each audit record at least the following information: [Assignment: *list of information included in audit records.*]

7.1.2 Class FPT: Protection of the TSF

7.1.2.1 FPT_TRC.X: Internal TSF data subset Consistency

Hierarchical to: No other components

Dependencies: FPT_ITT.1

FPT_TRC.X is a subset refinement to FPT_TRC.1.

FPT_TRC.X.1 The TSF shall ensure that [Assignment: *subset of the TSF data that must be consistent*] is consistent when replicated between parts of the TOE.

FPT_TRC.X.2 When parts of the TOE containing replicated [Assignment: *subset of the TSF data that must be consistent*] are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [Assignment: *list of functions dependent on subset TSF data replication consistency*].

8 Conformance Claims

No conformance claim to a PP is made for Oracle Business Intelligence Enterprise Edition.

Annex A Rules for Group Privilege and Permissions Inheritance

A.1 Rules for Inheritance in Oracle BI Presentation Services

- Any permissions or privileges given explicitly to a user override any permissions or privileges inherited from the Presentation Services group to which the user belongs.
- If a user belongs to two groups and both groups are assigned permissions, the least restrictive permissions are given to the user.

For example, if one group allows Read access and another allows Change access, the least restrictive access would be granted; in this example, Change access.

NOTE: The exception to this is if one of the two groups is explicitly denied the permissions, in which case the user is denied.

- If a user belongs to Presentation Services group X, and Presentation Services group X belongs to Presentation Services group Y, any rule assigned to group X overrides any rule assigned to group Y.
- For example, if Marketing has Read permissions, Marketing Administrators, which is a member of Marketing, can have Full Control permissions.
- Explicitly denying access takes precedence over any other permissions or privileges.

A.2 Example of Inherited Permissions and Privileges in Oracle BI Presentation Services

Figure A.1 shows an example of how privileges are inherited through Presentation Services groups.

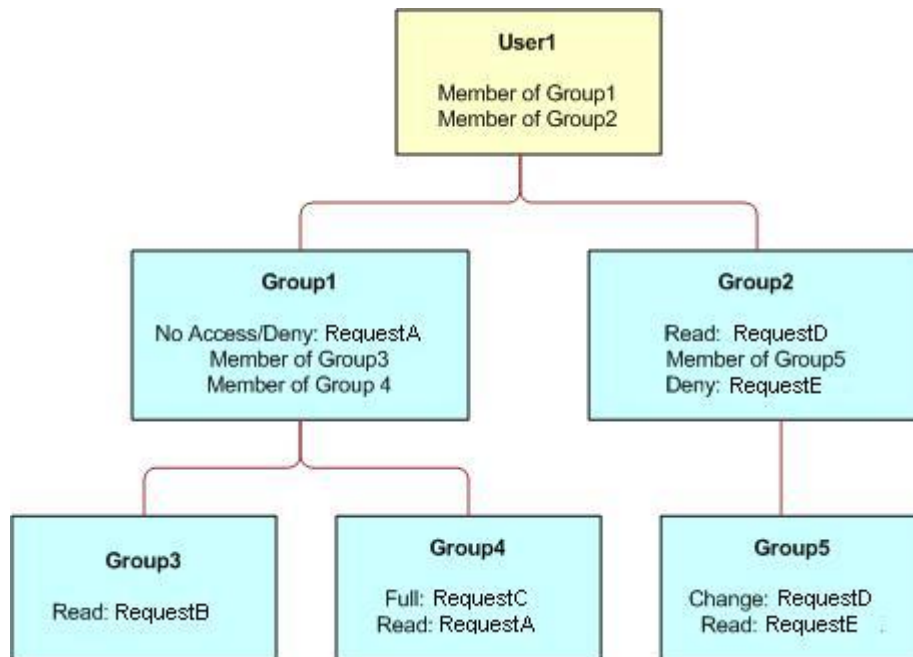


Figure A.1: Example of Privilege and Permission Inheritance

In this example:

- User1 is a direct member of Group 1 and Group 2, and is an indirect member of Group 3, Group 4, and Group 5.
- The permissions and privileges from Group 1 are no access to RequestA, Read access to RequestB, and Full Control over RequestC.
- If permissions and privileges are conflicting, the least restrictive level of authority is granted. Therefore, the inherited permissions and privileges from Group 2 include Change and Delete access to RequestD.
- Specifically prohibiting access always takes precedence over any other settings. Therefore, Group 1's denial of access to RequestA overrides Group 4's Read access. The result is that Group 1 provides no access to RequestA. Likewise, Group 5 provides no access to RequestE because access to it is explicitly denied in Group2.

The total permissions and privileges granted to User1 are as follows:

- No access to RequestA and RequestE because access is specifically denied.
- Read access to RequestB.

- Full Control over RequestC.
- Change and Delete access to RequestD.

Annex B Presentation Catalog Object Types List

This Annex provides a complete list of the presentation objects that are covered by the Presentation Objects Access Policy identified in FDP_ACC.1a and FDP_ACF.1a.

B.1 In scope of the TOE

Requests
Filters
Folders
Links

Present but restricted to the Presentation Services Administrator by ACL:

MetadataDocs
KeyValueMaps
Privileges
SecurityVersions
AccountIndexes
AccountDatas
SqlNodeCaches
GUIDStates
Replications

B.2 Out of scope of the TOE

The following object types are also covered by the **Presentation Object Access Policy**, but are not expected to actually be stored in the TOE because the products that could create them are out of scope of the TOE by privilege:

IBots
DeliveryProfiles
DefaultDevices
Subscriptions
DashboardDeliverys
DeviceMetrics
DisconnectedApplications
DisconnectedUserApplications
DisconenctedQueryTimeStamps
MarketingSegments
MarketingTrees
MarketingDefaults
MarketingExportFormats
MarketingExportFormatCampaigns

MarketingExportFormatLists
MarketingExportFormatAnalytics
MarketingExportFormatCustomers
MarketingExportFormatMailServers
MarketingExportFormatSavedResultSets
BriefingBooks
DashboardDeliveryContents
DashboardPrompts
DashboardLayouts
DashboardPages
DashboardSelections

Annex C

C.1 DELL Optiplex 745 hardware configuration

OPTIPLEX 745 MT - CORE 2 DUO E6400 (2.13

MEMORY : 2048MB (2X1024MB) 667MHZ DDR2 D

FLOPPY DISK DRIVE : NOT INCLUDED

HARD DRIVE : 250GB (7200RPM)3.5IN SERIAL

16X DVD+/-RW DRIVE

CYBERLINK SOFTWARE DECODE V5.7 BACKUP ME

SECURITY : CHASSIS INTRUSION SWITCH

SPEAKERS : INTERNAL SPEAKER

DELL 2 BUTTON USB SCROLL BLACK OPTICAL M

KEYBOARD : UK/IRISH (QWERTY) DELL ENHANC